What is claimed is:

1. A key management device for managing keys, the keys being grouped into a plurality of key groups each of which is assigned to one of a plurality of reproducing devices for decrypting encrypted data to reproduce the data, the key management device comprising:

key storage means for storing the keys, wherein

each key is associated with a node forming at least one N-layer tree structure (N is 2 or a natural number greater than 2), and

each key group includes keys associated with a different group of nodes, each group of nodes being a set of nodes located on a different path, in each tree structure, connecting a different node on the N^{th} layer and a node on the highest layer; and

encryption information generating means for, upon receipt of information designating a key group assigned to one of the reproducing devices,

(1) invalidating each key in the designated key group,

(2) selecting non-invalid keys being immediately subordinate to each invalid key from among keys in the key groups that are assigned to the other reproducing devices and each of which includes one or more invalid keys, and

(3) generating encryption information that includes (i) ciphertexts corresponding to a content key that is used to

encrypt the data, the ciphertexts being generated by encrypting the content key using each selected key, and (ii) identification information for identifying the selected keys, and wherein

each reproducing device stores *N* keys assigned thereto, selectively decrypts one of the ciphertexts that is decryptable using a key identified by the identification information to obtain the content key, and decrypts the data using the thus obtained content key to reproduce a content.

2. The key management device of Claim 1, wherein

the encryption information generating means includes:

a data generating unit which generates the data by encrypting the content using the content key;

an invalid key accepting unit which accepts the information designating the key group assigned to the one reproducing device;

a key selecting unit which invalidates each key in the designated key group, and selects the non-invalid keys being immediately subordinate on a different path to each invalid key except for the invalid key residing on the N^{th} layer;

a ciphertext generating unit which generates the ciphertexts by encrypting the content key using each selected key; and

a selected key list generating unit which generates a list used to identify the selected keys.

3. The key management device of Claim 2, wherein

the key storage means includes a key management information

storage unit which stores each key's (i) identifier for identifying the key, (ii) parent key identifier for identifying its parent key being immediately superordinate to the key, (iii) key state information showing whether the key is a selected key being used to generate one of the ciphertexts, an invalid key, or a non-used key, and (iv) key data, and

the invalid key accepting unit accepts identifiers for each key in the designated key group, and

the key selecting unit

(1) updates the key state information so as to invalidate a key of which identifier matches any of the designated identifiers, and

(2) updates the key state information so as to select a key (i) of which identifier does not match any of the designated identifiers, (ii) of which parent key is invalidated, and (iii) that is neither invalided nor selected.

4. The key management device of Claim 3, wherein

in the key management information, the key on the highest layer has a specific value as its parent key identifier, and

the key selecting unit selects the key of which parent identifier has the specific value as a selected key unless the key is invalidated.

5. The key management device of Claim 2, wherein the encryption information generating means further includes:

a restoring key accepting unit which accepts information

designating a key group that has been invalidated and to be restored; and

a restoring unit which

(a) selects, from among the keys in the designated key group to be restored, a key of which parent key being immediately superordinate to the key and a brother key having the same parent key are both invalidated, and

(b) changes a subordinate key of the thus selected key in the designated key group to a non-used key.

6. The key managing device of Claim 5, wherein

the key storage means includes a key management information storage unit which stores, each key's (i) identifier for identifying the key, (ii) parent key identifier for identifying its parent key being immediately superordinate to the key, (iii) key state information showing whether the key is a selected key being used to generate one of the ciphertexts, an invalid key, or a non-used key, and (iv) key data,

the restoring key accepting unit accepts identifiers for each key in the designated key group to be restored, and

the restoring unit updates the key state information so as to

(1) select, from among keys having an identifier that matches any of the designated identifiers, (i) the key on the highest layer when its immediately subordinate key residing on a different path is currently selected, or (ii) a key on the second layer or below when its brother key having the same parent

key is all invalidated,

(2) change to a non-used key a key having an identifier that matches any of the designated identifiers and being subordinate on the same path to the thus selected key, and

(3) change to a non-used key a key having an identifier that does not match any of the designated identifiers and having the thus selected key as its parent key.

7. The key management device of Claim 2, further comprising:

new key accepting means for accepting the number of reproducing devices to which a key group is newly assigned;

new key generating means for generating keys which are associated with nodes forming an M-layer tree structure (M is a natural number between 2 and N inclusive); and

connecting means for replacing a key on the highest layer of the newly generated tree structure with a selected key or a non-used key residing on the $(N-M+1)^{th}$ or higher layer of the existing tree structure stored in the key recording means.

8. The key management device of Claim 2, further comprising recording means for recording to a recording medium the data generated by the data generating unit, the ciphertexts generated by the ciphertext generating unit, and the selected key list generated by the selected key generating unit.

9. The key management device of Claim 2, further comprising

transmitting means for transmitting to the plurality of reproducing devices the data generated by the data generating unit, the ciphertexts generated by the ciphertext generating unit, and the selected key list generated by the selected key generating unit.

10. The key management device of Claim 3, wherein

the key management information storing unit stores the key management information every time it is updated by the key selecting unit, and

the key storage means further includes a restoring unit for restoring the key management information back to its initial version or any updated version.

11. The key management device of Claim 1, wherein

the key storage means stores L tree structures, L being 2^{K+1} when the maximum number of key groups to be invalidated is set at 2^{K}.

12. A recording medium to be reproduced by one of a plurality of reproducing devices each of which stores a key group, wherein

each key in the key group being assigned to a node forming an N-layer tree structure (N is 2 or a natural number greater than 2) together with nodes with which keys stored in the other reproducing devices are associated, and

the keys in the key group being associated with a group of nodes that is a set of nodes located on a path, in each

tree structure, connecting a node on the N^{th} layer and a node on the highest layer,

the recording medium comprising:

a data area which stores data generated by encrypting a content using a content key;

a ciphertext area which stores at least one ciphertext generated by encrypting the content key using a selected key, the selected key being identical to one of the keys stored in each reproducing device except for a specifically designated reproducing device; and

a selected key list area which stores information identifying the selected key used for encrypting the content key.

13. A reproducing device for decrypting encrypted data to reproduce the data, the reproducing device comprising:

key group storing means for storing N keys (N is 2 or a natural number greater than 2), wherein

the N keys are respectively associated with nodes forming an N-layer tree structure together with nodes with which keys stored in other reproducing devices are associated, and

the N keys are associated with a group of nodes that is a set of nodes located on a path, in the tree structure, connecting a node on the N^{th} layer to a node on the highest layer;

reproduction information obtaining means for obtaining (i) the data by encrypting a content using a content key, (ii) at least one ciphertext generated by encrypting the content key,

and (iii) identification information for identifying a key used to encrypt the content key;

content key decrypting means for selecting a key identified by the identification information from the keys stored in the key group storage means, and decrypting the ciphertext that is decryptable using the thus selected key to obtain the content key; and

content reproducing means for decrypting the data using the thus obtained content key to reproduce the content.

14. The reproducing device of Claim 13, further comprising read means for reading from a recording medium (i) the data generated by encrypting the content using the content key, (ii) the ciphertext generated by encrypting the content key, and (iii) the information for identifying the key used to decrypt the content key, and passing the read result to the reproduction information obtaining means.

15. The reproducing device of Claim 13, further comprising receiving means for receiving (i) the data generated by encrypting the content using the content key, (ii) the ciphertext generated by encrypting the content key, and (iii) the information for identifying the key used to decrypt the content key, and passing the received result to the reproduction information obtaining means.

16. A key management method for use in a key management device

to manage keys stored in a storage area of the key management device, wherein

the keys are grouped into a plurality of key groups each of which is assigned to one of a plurality of reproducing devices,

each key is associated with a node forming at least one N-layer tree structure (N is 2 or a natural number greater than 2),

each key group includes keys associated with a different group of nodes, each group of nodes being a set of nodes located on a different path, in each tree structure, connecting a different node on the N^{th} layer and a node on the highest layer, the key management method comprising:

an accepting step for accepting information designating a key group stored in one of the reproducing devices;

a key selecting step for

(1) invalidating each key in the designated key group, and

(2) selecting non-invalid keys being immediately subordinate to each invalid key from among keys in the key groups that are assigned to the other reproducing devices and each of which includes one or more invalid keys; and

an encryption information generating step for generating encryption information that includes (i) ciphertexts corresponding to a content key that is used to encrypt the data, the ciphertexts being generated by encrypting the content key using each selected key, and (ii) identification information

for identifying the selected keys, and wherein

each reproducing device stores N keys assigned thereto, selectively decrypts one of the ciphertexts that is decryptable using a key identified by the identification information to obtain the content key, and decrypts the data using the thus obtained content key to reproduce a content.

17. A key management program for use in a computer to manage keys, the keys being grouped into a plurality of key groups each of which is assigned to one of a plurality of reproducing devices, wherein

each key is associated with a node forming at least one N-layer tree structure (N is 2 or a natural number greater than 2),

each key group includes keys associated with a different group of nodes, each group of nodes being a set of nodes located on a different path, in each tree structure, connecting a different node on the N^{th} layer and a node on the highest layer, the program comprising:

an accepting step for accepting information designating a key group stored in one of the reproducing devices;

a key selecting step for

(1) invalidating each key in the designated key group, and

(2) selecting non-invalid keys being immediately subordinate to each invalid key from among keys in the key groups that are assigned to the other reproducing devices and each of

which includes one or more invalid keys; and

an encryption information generating step for generating encryption information that includes (i) ciphertexts corresponding to a content key that is used to encrypt the data, the ciphertexts being generated by encrypting the content key using each selected key, and (ii) identification information for identifying the selected keys, and wherein

each reproducing device stores N keys assigned thereto, selectively decrypts one of the ciphertexts that is decryptable using a key identified by the identification information to obtain the content key, and decrypts the data using the thus obtained content key to reproduce a content.

18. A computer readable recording medium for use in a key management device to manage keys, the keys being grouped into a plurality of key groups each of which is assigned to one of a plurality of reproducing devices, wherein

each key is associated with a node forming at least one N-layer tree structure (N is 2 or a natural number greater than 2),

each key group includes keys associated with a different group of nodes, each group of nodes being a set of nodes located on a different path, in each tree structure, connecting a different node on the N^{th} layer and a node on the highest layer, the recording medium comprising:

an accepting step for accepting information designating a key group stored in one of the reproducing devices;

a key selecting step for

(1) invalidating each key in the designated key group, and

(2) selecting non-invalid keys being immediately subordinate to each invalid key from among keys in the key groups that are assigned to the other reproducing devices and each of which includes one or more invalid keys; and

an encryption information generating step for generating encryption information that includes (i) ciphertexts corresponding to a content key that is used to encrypt the data, the ciphertexts being generated by encrypting the content key using each selected key, and (ii) identification information for identifying the selected keys, and wherein

each reproducing device stores *N* keys assigned thereto, selectively decrypts one of the ciphertexts that is decryptable using a key identified by the identification information to obtain the content key, and decrypts the data using the thus obtained content key to reproduce a content.

19. A system comprising:

a plurality of recording devices for recording encrypted data to a rewritable recording medium;

a plurality of reproducing devices for decrypting and reproducing the encrypted data being recoded in the recording medium; and

a key management device for managing keys, the keys being grouped into a plurality of key groups each of which is assigned

to the plurality of recording devices and the plurality of reproducing devices, wherein

the key management device includes:

key storage means for storing the keys, wherein

each key is associated with a node forming at least one N-layer tree structure (N is 2 or a natural number greater than 2), and

each key group includes keys associated with a different group of nodes, each group of nodes being a set of nodes located on a different path, in each tree structure, connecting a different node on the N^{th} layer and a node on the highest layer;

encryption information generating means for, upon receipt of information designating a key group assigned to one of the recording devices and/or one of the reproducing devices,

(1) invalidating each key in the designated key group,

(2) selecting non-invalid keys being immediately subordinate to each invalid key from among keys in the key groups that are assigned to the other recording devices and/or the other reproducing devices and each of which includes one or more invalid keys, and

(3) generating encryption information that includes (i) at least one ciphertext corresponding to a content key that is used to encrypt the data, the ciphertexts being generated by encrypting the content key using each selected key, and (ii) identification information for identifying the selected keys;

and

encryption information recording means for recording the thus generated encryption information to the recording medium,

each recording device includes:

key group storing means for storing N keys, the N keys being associated with nodes located on a path, in each tree structure, connecting a node on the N^{th} layer to a node on the highest layer;

content key decrypting means for reading the encryption information from the recording medium, identifying a key stored in the key group storing means using the identification information, and decrypting the ciphertext being decryptable with the thus identified key to obtain the content key; and

content encrypting means for encrypting a content using the thus obtained content key, and record the resulting encrypted data to the recording medium, and

each reproducing device includes:

key group storing means for storing N keys, the N keys being associated with nodes located on a path, in the tree structure, connecting a node on the N^{th} layer to a node on the highest layer;

reproduction information obtaining means for obtaining the data generated by encrypting the content using the content key, the ciphertext generated by encrypting the content key, and the identification information for identifying the key used to encrypt the content key;

content key decrypting means for selecting a key identified

by the identification information from the keys stored in the key group storage means, and decrypting the ciphertext decryptable using the thus selected key to obtain the content key; and

content reproducing means for decrypting the data using the thus obtained content key to reproduce the content.

20. A rewritable recording medium having data generated by encrypting a content using a content key, the data being recorded by a recording device storing one of key groups, and read/reproduced by a reproducing device storing one of the key groups, wherein

the key groups together include keys each of which is associated with a node forming an N-layer tree structure (N is 2 or a natural number greater than 2),

each key group includes keys associated with a different group of nodes, each group of nodes that is a set of nodes located on a different path, in the tree structure, connecting a different node on the N^{th} layer and a node on the highest layer, the recording medium comprising:

a ciphertext area for storing at least one ciphertext generated by encrypting the content key using a selected key, the selected key being identical to a key stored in the recoding device and a key stored in the reproducing device;

a selected key area for storing identification information identifying the selected key used for encrypting the content key; and

a data area for storing data recorded by the recording device, the data being decryptable using the content key, the content key is obtained by decrypting the ciphertext using the key that is stored in the reproducing device and selected according to the identification information.

21. A key management device for managing keys, the keys being grouped into a plurality of key groups each of which is assigned to one of a plurality of recording devices for recording encrypted data in a rewritable recording medium, and to one of a plurality of reproducing devices for decrypting the encrypted data recorded in the recording medium to reproduce the data, the key management device comprising:

key storing means key storage means for storing the keys, wherein

each key is associated with a node forming at least one N-layer tree structure (N is 2 or a natural number greater than 2), and

each key group includes keys associated with a different group of nodes, each group of nodes being a set of nodes located on a different path, in each tree structure, connecting a different node on the N^{th} layer and a node on the highest layer;

encryption information generating means for, upon receipt of information designating a key group assigned to one of the reproducing devices,

(1) invalidating each key in the designated key

group,

(2) selecting non-invalid keys being immediately subordinate to each invalid key from among keys in the key groups that are assigned to the other reproducing devices and each of which includes one or more invalid keys, and

(3) generating encryption information that includes (i) ciphertexts corresponding to a content key that is used to encrypt the data, the ciphertexts being generated by encrypting the content key using each selected key, and (ii) identification information for identifying the selected keys; and

encryption information recording means for recording the thus generated encryption information in the recording medium.

22. A recording device for recording encrypted data in a rewritable recording medium, the recording device comprising:

key group storing means for storing N keys (N is 2 or a natural number greater than 2), wherein

the N keys are respectively associated with nodes forming an N-layer tree structure together with nodes with which keys stored in other recording devices are associated, and

the N keys are associated with a group of nodes that is a set of nodes located on a path, in the tree structure, connecting a node on the N^{th} layer to a node on the highest layer;

content key decrypting means for reading the encryption information from the recording medium, selecting a key stored in the key group storing means using identification information, and decrypting a ciphertext being decryptable with the thus

selected key to obtain the content key, wherein

the recording medium pre-stores encryption information including at least the ciphertext encrypted using the selected key and the identification information for identifying the selected key; and

content encrypting means for encrypting a content using the thus obtained content key, and record the resulting encrypted data to the recording medium.